

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 04-05-2013		2. REPORT TYPE Master of Military Studies Research Paper		3. DATES COVERED (From - To) August 2012 - April 2013	
4. TITLE AND SUBTITLE Cyber Warfare: An Evolution in Warfare not Just War Theory				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) Yates, Joel A. Lieutenant Commander, USN				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSOR/MONITOR'S ACRONYM(S) N/A	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES N/A					
14. ABSTRACT As the Internet increasingly allows people, businesses, governments, militaries, and organizations to network computing systems, it also opens an avenue for nefarious actors to wage cyber attacks against all who use the Internet. National infrastructures, government and military systems, and financial institutions that operate as networked systems are vulnerable to cyber attacks. Nation-states or non-state actors that threaten the security of other nation-states by cyber attacks can cause lethal effects that must be evaluated for the ethical and moral impacts. The Just War Theory has played a large role in evaluating the ethical and moral use of new weapons throughout history; cyber is not different. The application of Just War Theory to cyber warfare is greatly debated. While some argue that Just War Theory is irrelevant to cyber warfare, a careful analysis demonstrates that it is a useful tool for considering the morality of cyber warfare. This paper examines the application of Just War Theory to cyber warfare and contends that Just War Theory is a useful tool for considering the morality of cyber warfare.					
15. SUBJECT TERMS Cyber Attack, Cyber Warfare, Just War Theory, Just Cause, Proportionality, Probability of Success, Ethics, Attribution					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 34	19a. NAME OF RESPONSIBLE PERSON Marine Corps University/Command
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (include area code) (703) 784-3330 (Admin Office)

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

TITLE:

Cyber Warfare:
An Evolution in Warfare not Just War Theory

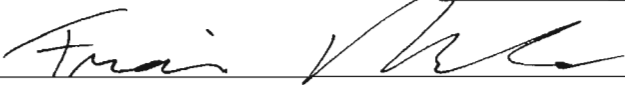
SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

LCDR Joel A. Yates, U.S. Navy

AY 12-13

Mentor and Oral Defense Committee Member: Dr. Francis H. Marlo

Approved: 

Date: 4 April 2013

Oral Defense Committee Member: Dr. Rebecca J. Johnson

Approved: 

Date: 4 April 2013

Executive Summary

Title: Cyber Warfare: An Evolution in Warfare not Just War Theory

Author: Lieutenant Commander Joel Yates, United States Navy

Thesis: While some argue that Just War Theory is irrelevant to cyber warfare, a careful analysis demonstrates that it is a useful tool for considering the morality of CW.

Discussion: Though nations have a right to self-defense, there are constraints and limitations to the actions that can be taken in that effort. New warfare areas throughout the history of war, whether nuclear warfare or air warfare, underwent debates of whether their use was ethical; CW is no different. With a cyberspace that knows no physical boundaries, it is important to understand the ethical implications of CW that includes touching, disabling, degrading, denying the use of, or destroying distant computing systems in the interest of protecting national security. There are many facets to understanding the ethical implication of such operations. Most of those facets are being debated under the question of whether JWT, in its original form, suffices as an accurate ethical measurement for cyber operations. This paper analyzes the two camps and provides evidence to the reasons why JWT applies to CW.

Conclusion: As long as the U.S. applies the JWT criterion when confronted with a decision to respond to the threat or use of force by an antagonist, the weapon it chooses to deploy is secondary to the justification.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

Page

Figure 1. 2012 Cyber Attack Distribution	9
--	---

Preface

This Master of Military Science (MMS) paper is an analysis of the application of Just War Theory to Cyber Warfare. As government and civilian organizations continue to increase their dependency on networked computers that control communications, infrastructures, and weapons systems, the vulnerabilities of exploitation, manipulation, and corruption likewise increase. The threat to national security presented by these vulnerabilities challenges nation-states to determine whether Just War Theory is applicable to Cyber Warfare.

As a Navy Information Warfare Officer with a working knowledge of Cyber Warfare within the Navy, an exploration of the Just War Theory debate seemed a worthwhile undertaking, particularly when the U.S. Government is positioned to conduct cyber operations in defense of the national security. While I may understand the operations in cyber to some degree and have experience in Cyber Warfare, I have no experience in international law or Just War Theory outside of my limited understanding obtained through the research of this paper and course work at the United States Marine Corps Command and Staff College. I have however, received a considerable amount of support, assistance, and guidance from: Dr. Francis H. Marlo, PhD in Political Science, Associate Professor of National Security Affairs, U.S. Marine Corps Command and Staff College; Dr. Rebecca J. Johnson, PhD in International Relations, Associate Professor of National Security Affairs, U.S. Marine Corps Command and Staff College; Mr. Steve Hendricks, Senior Intelligence Officer, Naval Air Systems Command, and Professor of Technical Management in the Master's in Systems Engineering and Technical Management program at Whiting School of Engineering, Johns Hopkins University. I owe these mentors a huge debt of gratitude for their support, guidance, and honest feedback during this period of educational growth. More importantly, I am thankful for the patience and motivation my spouse so graciously provided me.

Table of Contents

	Page
EXECUTIVE SUMMARY	i
DISCLAIMER	ii
LIST OF ILLUSTRATIONS	iii
PREFACE	iv
INTRODUCTION	1
EXAMINATION OF COMPETING ARGUMENTS	9
CONCLUSIONS	21
CITATIONS	23
BIBLIOGRAPHY	25

Chapter One INTRODUCTION

The Internet created an exponential change to the speed of communications and enabled near instantaneous sharing of information across the globe. In many cases, this change greatly improved global business interactions and military operations, and allowed people to interact socially regardless of their location. As the Internet use continues to grow, nation-states are becoming more dependent on access to it for military operations, management and operation of critical infrastructure, and business interactions. However, along with these enormous benefits, the Internet has also created an avenue for individuals (hacktivists^{*}), organizations (such as terrorist or criminal groups), businesses, and nation-states to conduct harmful cyber warfare (CW). While some argue that Just War Theory (JWT) is irrelevant to CW, a careful analysis demonstrates that it is a useful tool for considering the morality of CW.

Anyone connected to the Internet can conduct CW against governments or civilians because of the wide availability of simple hacking toolkits. Though individuals with simple hacking tools or elementary knowledge of computers can pose threats, they are typically not threats that would rise to the level of national security concerns. The more sophisticated cyber attacks that are most threatening to nation-states require significant financial backing, organization, and intellectual capital. These sophisticated attacks are normally committed by nation-states or well-organized non-state actors.

To give some perspective on the above threats on the Internet, the following two actual cyber attacks illustrate the difference between a less advanced and more sophisticated cyber attack.

1. A 15-year old Austrian boy hacked 259 websites between January and March 2012.

His hacking skills and knowledge were nominal at best prior to him pulling down a

^{*} A person who engages in *hacktivism*, which is the act of hacking into a Web site or computer system in order to communicate a politically or socially motivated message.

prepackaged set of hacking tools from the Internet. His hacking ignorance led to him leaving his Internet Protocol (IP) signature in the tools when he launched his attack on the web sites. Police detected the IP error and prosecuted the boy.¹ The level of damage he caused was relatively minor and probably amounted to lost revenues and customer trust by the businesses that were hacked. His success was the result of the relative ease of access to online hacking tools and the ease in exploiting holes in the servers hosting the web sites. The success of the attack had nothing to do with the intellectual capital, financial backing, or organization of his attack, and it posed little threat to any country's national security.

2. In late 2009, and again in mid 2011, Google was the victim of sophisticated cyber attacks that succeeded in defeating its elaborate system security protocols. The attackers gained access to source code and Gmail user accounts of senior U.S. officials and human rights activists. Although Google suspected China for the attacks, Google officials are careful not to attribute the attack directly to China.² Nevertheless, the level of sophistication involved in the attack required intellectual capital, persistence on gathering intelligence of Google's vulnerabilities, and financial support. Though this attack was not necessarily a threat to national security, if a similarly capable entity (nation-state or otherwise) targeted a critical network that supported another nation-state's power, water, financial markets, or military operations with the same level of sophistication and found success, it could create a national security emergency.

Both of the examples could pose potential national security threats to governments that are increasingly dependent on networked military, financial, and infrastructure operations. Though the first scenario presented little threat based on the goals and intent of the young 15-year old boy, if he intended to target government websites or other IP-supported organized services, and

those sites were similarly vulnerable, the impact of denying the services provided by those web sites may be extremely damaging to national security.

The increased government employment of IP-networked systems throughout the globe has sparked a debate on how to manage and control activity on the Internet in the interest of minimizing the risks to the critical infrastructures, financial markets, and military operations. In parallel to debates on international policy and acceptable norms of Internet conduct, a debate is ongoing as to whether it is ever ethical for a nation to use cyber attacks against another nation. Whether norms and follow-on policies are ever established, nations must take measures to defend their people, financial well-being, and military capabilities.

Although nations have a right to self-defense, there are constraints and limitations to the actions they can take in that effort. New warfare areas throughout the history of war, whether nuclear warfare or air warfare, underwent scrutiny on the constraints and limitations of their ethical use; Cyber Warfare is no different. Conventional weapons systems are more accurate, wirelessly controlled through IP connections, and process more information than ever before, which makes them inherently vulnerable to CW. Civilian critical infrastructure, banking, and medical systems are equally vulnerable when controlled and managed through Internet IP schema. With that in mind, there are ethical concerns with CW that targets weapons systems, civilian critical infrastructure, and other IP-controlled systems.

There are many facets to understanding the ethical implication of such operations. With a cyberspace that knows no physical boundaries, it is important to understand these facets of CW that includes touching, disabling, disrupting, degrading, denying the use of, or destroying distant computing systems in the interest of protecting national security. Most of those facets are argued under the question of whether JWT, in its original form, suffices as an accurate ethical

measurement for cyber operations.

Two of the major bodies of JWT are *jus ad bellum* and *jus in bello*. The *jus ad bellum* body addresses the morality of war and is the concept that the initiation of war must be within a just cause, right authority, last resort, probability of success, proportionality, and with the aim of peace. Nations may be justified in initiating war within one of two situations. First, a nation has the right to self-defense in response to a use of force against it. Secondly, if a nation interprets another nation's rhetoric and actions as a threat to use force against it, it may be justified in launching a preemptive strike in order to deter or eliminate the threat from the opposing nation.

The second body of JWT is *jus in bello*. It deals with the morality in war between nations. Once the nations are actively at war, there are parameters of ethically conducting the war and using force. The employment of force must be directly related to providing a military advantage in the war and not just destroying whatever is in the path of the advance indiscriminately. It provides a means to measure the morality of the employment of force within the war, whereby that employment can be judged for its application to affect the opponent's ability to continue the fight.

The JWT application to CW is being debated over the *jus ad bellum* and *jus in bello* bodies. This paper will focus on the first aforementioned situation in *jus ad bellum* and the *jus in bello* bodies to understand the two competing arguments. Moreover, this paper will use the JWT criterion of just cause, probability of success, and proportionality.

Prior to discussing the arguments on both sides of the ethical debate, it is important to understand what cyberspace is and what the international and U.S. government positions are on CW. The U.S. Joint Publication 1 (Doctrine for the Armed Forces of the United States) defines cyberspace as “a global domain within the information environment consisting of the

*interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”*³

This paper will use this definition, because it encompasses the physical and informational nature of cyber. Cyberspace is not simply a virtual “cloud” of information transmitted through binary code that is difficult to touch. It includes the physical aspects of the systems that interconnect through the IP schema, as well as the intangible operating systems (OS), software, and information held within the hardware.

The physical aspects, OS, software, and information are all targets for exploitation, corruption, and manipulation. The nations, groups, or individuals that take advantage of these vulnerabilities can present threats to peace, breaches of peace, and acts of aggression, as the 15-year old Austrian and Google incidents demonstrate. These threats and breaches of peace, and acts of aggression require evaluation for their ethical significance.

The U.S. Government is posturing itself to respond to any threat or breach of peace, or act of aggression. In the May 2011 *International Strategy for Cyberspace*, President Barrack Obama stated, "When warranted, we will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests."⁴ With this statement, the U.S. indirectly asserted its position that hostile acts in cyberspace, which are cyber attacks, are "armed attacks" and positioned itself under the U.N. Article 51[†] umbrella of self-defense.

[†] Article 51: Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. United Nations, *Charter of the United Nations and Statute of the International Court of Justice*. (New York; UN Publications, 2013).
<http://www.un.org/en/documents/charter/chapter7.shtml>.

Furthermore, the U.S. Department of Defense (DoD) has postured itself to respond to calls for military options from the President. In June 2009, DoD directed the establishment of the U.S. Cyber Command (USCYBERCOM) under U.S. Strategic Command (USSTRATCOM). In October 2010, USCYBERCOM reached full operational status. It is responsible for synchronizing and coordinating Service components within each branch of the military, including U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. TENTH Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command and U.S. Coast Guard Cyber Command.⁵ The commander of USCYBERCOM is also the director of the National Security Agency. That "dual-hatting" provides close coordination and information sharing across the respective subordinate units. The arrangement ties the nation's top signals intelligence (SIGINT) organization with the nation's cyber-focused military command in a symbiotic relationship.

The recent efforts by the U.S. government to establish a distinct military command structure, strategy, and guidance toward cyberspace and operations are evidence that it thinks the potential for cyber conflicts is high. Indeed, the U.S. has already acknowledged that it has conducted cyber attacks. In May 2012 then-Secretary of State, Hillary Clinton openly admitted that the U.S. conducted cyber attacks against Al Qaeda networks in Yemen.⁶ This confession to active cyber operations from the U.S. is proof to the international community that the U.S. is backing up the new cyber organization, strategy, and doctrine with actions. It also provided the evidence that the U.S. is defending itself within cyberspace.

Nonetheless, the question of JWT applicability remains heavily debated within the U.S. The manipulation of the OS and software through vulnerabilities, hidden or known, can cause damage to computing system's physical components and any ancillary equipment or systems. Additionally, software accessed through vulnerabilities may be controlled, reprogrammed, or

made ineffective. This physical, OS, and software manipulation can subsequently affect systems that are reliant on the computer to operate. Military weapons systems, life-sustaining hospital equipment, city power grids, water treatment plants, and traffic control mechanisms that are manipulated by cyber weapons can cause lethal effects to human beings. There are several ethical implications to targeting civilian systems, and the assessment of those ethical implications are why ethical reasoning should be applied to cyber operations.

Military and civilian academics are reviewing JWT because its application to CW is being questioned. On one side of the debate are scholars such Dr. Patrick Lin[‡], Dr. Fritz Allhoff[§], and Dr. Neil Rowe.^{**7} The three argue that JWT is not adequate for application to CW. They lean on a traditional view of JWT that contends that the JWT only applies to aggression that risks human life.⁸ Their assertions depend on the principle that cyber weapons are only weapons against information and data, but are not a part of warfare that injures or kills human beings.

Another critic of JWT's application to CW is Dr. Randall Dipert.^{††} He evaluated the JWT through the typical six criteria of *jus ad bellum*.⁹ His argument is that JWT must undergo a makeover to be applicable to CW. He, like Lin, Allhoff, and Rowe, leans on the premise that cyber weapons are not capable of threatening human life and therefore cannot be evaluated for their ethical and moral use under the JWT.

The counter argument is that JWT, as it has in many historical cases of new weaponry, is capable of assessing CW without undergoing a transformation. Colonel James Cook^{‡‡}, Dr.

[‡]Dr. Lin is an Associate Professor of Philosophy, and Director of the Ethics and Emerging Sciences Group at California Polytechnic State University.

[§] Dr. Allhoff is an Associate Professor of in the Department of Philosophy at Western Michigan University, and a Senior Research Fellow at The Australian National University's Centre for Applied Philosophy and Public Ethics.

^{**} Dr. Rowe is a Professor of Computer Science at the Naval Postgraduate School.

^{††} Dr. Dipert is a professor at the State University of New York, Buffalo.

^{‡‡} Colonel Cook is a Professor at the U.S. Air Force Academy.

Roger Crisp^{§§}, and Captain (Retired) Maxie Davis^{***} argue that CW can be lethal. The three dispute the theory that the six categories of JWT are not useful in measuring CW actions to determine their ethical and just use.

The focus of this paper is to analyze both arguments. In the end, this paper will attempt to show that cyberspace is a medium capable of launching cyber weapons that cause lethal effects on human beings, equipment, and virtual data. Upon establishing that argument, the application of JWT to CW should be evident.

^{§§} Dr. Crisp is a Professor at St. Anne's College of Oxford

^{***} Captain (Retired) Davis is the Deputy Information and Technology Services for the Department of Navy and retired US Navy Captain.

Chapter Two

EXAMINATION OF COMPETING ARGUMENTS

To begin this examination, it is important to put into perspective the number of reported cyber attacks occurring annually. The breakdown of cyber attacks for 2012 is shown in Figure 1, which illustrates the small percentage of attacks that would break the threshold of threats to national security.¹⁰ It is important to understand that this chart only reflects reported cyber attacks - there are certainly more that go unreported.

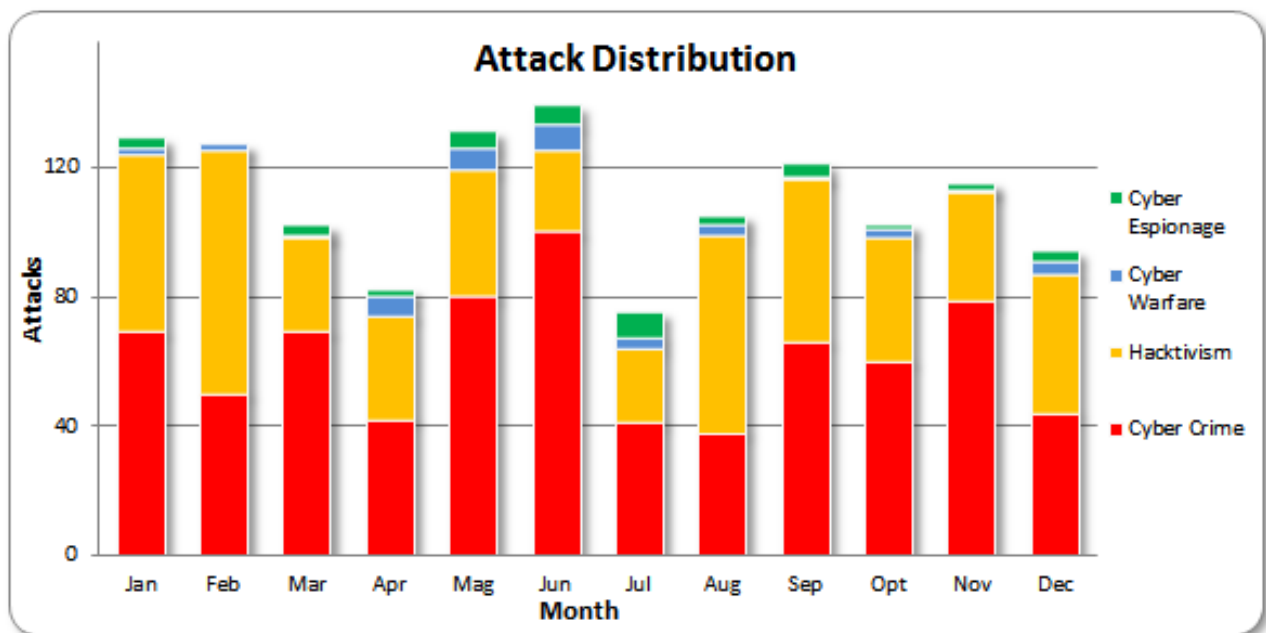


Figure 1

As the chart depicts, the majority of cyber attacks are pure Cyber Crimes and Hacktivism. Far less of the cyber attacks are Cyber Espionage and Cyber Warfare. Though Cyber Espionage and Cyber Warfare are a small number of the overall cyber attacks, they represent the largest threats to national security because of their potential to target military operations, critical infrastructure, medical services, financial institutions, and mass transit systems.

CW's potential to inflict harm to a level that would justify a responding attack with a cyber or conventional weapon is at the center of the debate. The arguments on both sides are focus on

three primary areas: just cause, probability of success, and proportionality. This chapter will breakdown the differences within the debates based on these three categories.

JUST CAUSE

Just cause in JWT is the premise that a state or nation can use force when it is in “self-defence from external attack; the protection of innocents; and punishment for wrongdoing.”¹¹ It does not mean that in the absence of credible hostile threats or aggression that a state can be justified in using preemptive, preventative, or responding strikes against another nation. For a response to threats or the use of force to be within the just cause criterion, the nation targeted by the aggression must be credibly threatened or wronged by the aggressor nation. In other words, if a state resorted to war in response to aggression from another state in order to protect itself and its citizens from attack or to right the wrong from a previous aggression, the responding state would satisfy the just cause body of JWT.

- Argument against CW creating a “just cause”

The case that Dipert, Lin, Allhoff, and Rowe make against the application of JWT to CW is based partly on their belief that cyberspace, and by extension cyber attacks, cannot cause physical harm or death to humans. In fact, Dipert argues that “[cyberwarfare] differ from previous forms of warfare in neither injuring nor killing human beings, nor causing lasting physical damage - but can nevertheless cause serious harm to a nation's vital interests.”¹² Others argue similarly that, “If aggression in cyberspace is not tied to actual physical harm or threat to lives, it is unclear then how we should understand it.”¹³

The argument made by this camp is that a “just war” is one waged when human life or massive destruction is threatened, or if a use of force has already caused loss of human life or massive destruction. However, they concede that cyber attacks can have second or third order

effects that could cause loss of life or massive destruction, but that CW is never the first order effect and therefore isn't a directly lethal weapon.¹⁴ The assertion is that CW cannot cause a loss of life or massive destruction, and therefore could not create a just cause for war, and by inclusion, is not covered by JWT.

- Rebuttal

Justifying war or acts of aggression in any warfare area is complex and ambiguous, but that doesn't preclude the use of JWT to ensure the greater intent of self-defense is met. Cook argues that CW is not dissimilar to other types of warfare throughout history in that they all possessed ambiguities that did not invalidate JWT.¹⁵ Additionally, just because cyber weapons have not been used to cause a death does not mean that they are incapable of doing so. In fact, Dipert, himself presents a scenario in which cyber weapons could hypothetically cause death.

Dipert admits there are "sophisticated computerized weapons systems" that are susceptible to cyber attack.¹⁶ Using his example of the U.S. Navy's Aegis system, which is an anti-aircraft and anti-missile radar system and linked to missile systems that are designed to defeat aircraft and missiles, the harm to human beings is testable. Hypothetically, if a belligerent nation launched a cyber attack to exploit vulnerabilities in the computing systems of Aegis, the belligerent may be able to cause the missile system to fire on a civilian or military aircraft and hence cause a loss of life. The theory and argument that CW does not injure or kill human beings becomes exceptionally weak under that hypothetical problem. As a disclaimer, this author does not know whether Aegis is actually vulnerable to cyber attack. The point is not to confirm or deny Dipert's claims that it is vulnerable, but to show the potential lethality for harm through CW.

Furthermore, the DoD doesn't agree with any of the assessments that CW is incapable of harming human beings and has codified cyberspace as a military force-on-force operation within

traditional war:

Traditional war typically involves small-scale to large-scale, force-on-force military operations in which adversaries employ a variety of conventional military capabilities against each other in the air, land, maritime, and space physical domains and the information environment (which includes cyberspace).¹⁷

The codification of cyberspace as an element of conventional military capability provides evidence that the U.S. considers cyberspace, and by association CW, a battleground with the potential for lethal consequences. Ergo, CW threatened or used against the U.S. would constitute a “just cause” to respond and thereby the application of JWT to CW is appropriate.

PROBABILITY OF SUCCESS

When a state contemplates resorting to war, it may not meet the probability of success measure “[if] it can foresee that doing so will have no measureable impact on the situation.”¹⁸ In other words, “probability of success is always a matter of circumstance, of taking reasonable options within the constraints and opportunities presented by the world.”¹⁹ The probability of success criterion within JWT “[is] to bar lethal violence which is going to be futile.”²⁰ Target discrimination, developed from proper attribution, is critical to meeting the probability of success within the *jus ad bellum* and *jus in bello* bodies of JWT. Proper attribution provides legitimate targets that serve to perpetuate a solution to the conflict. Therefore, attacking a nation without adequately attributing it as the aggressor of attacks (cyber or conventional) may fail the probability of success criterion within JWT and create a scenario of futile lethality.^{†††}

Furthermore, proper attribution diminishes the civil liability and potential for international condemnation for unjust probability of success determination. All that discussed, ambiguities in

^{†††} I would like to thank Dr. Rebecca Johnson for suggesting this point in my work.

attribution are rarely decreased to zero and nations may decide the risk of not acting is greater than acting.

- Argument that originators of CW may not be identifiable

The camp opposing the application of JWT to CW highlights the problematic task of attributing a cyber attack to its originator. Therefore, without proper attribution CW fails to meet the probability of success within JWT. The assertion is that, "it is very difficult to determine the source of cyberattacks: this is the 'attribution problem'."²¹ Others further the discussion and explain, "[the] problem with cyberwarfare is that it is very easy to mask the identities of combatants."²² It is in fact, very difficult to attribute cyber attacks and therefore attacking a perceived aggressor incorrectly would lead to a probability of success issue.

Any nation, group, or individual Hactivist that targets a network for attack can conceal their identity from the victim of the attack. The methods of concealment are many, but here are a few to help understand the difficulty in tracing attacks:

1. Botnet method - a network of private computers infected with malicious software and controlled as a group without the owner's knowledge, e.g., to send spam. It can be used to launch a Distributive Denial of Service attack (DDOS).²³
2. IP spoofing - attacker obtains an IP address of a legitimate host and alters packets headers so that the legitimate host appears to be the source of an attack. The infected host can be used in a "zombie army" of computers to launch DDOS or malicious code, viruses, and worms.²⁴

The difficulty in tracking the origination of the attack can also be further complicated by the number of different servers that help route internet traffic globally. An attack may traverse

several country borders en route to its destination, which can complicate the tracking based on the different agreements in forensic tracking of internet incidents.

Some people suggest establishing international agreements to require digital signatures that would make tracking attacks easier.²⁵ Their argument is based on avoidance of collateral damage to civilians. Some argue to fix the attribution problem it may require a 'chip' or universal source identification be inserted in every computer.²⁶ In their argument, the probability of success in targeting the correct aggressor would be much greater.

- Rebuttal

Attributing the sources of CW threats is difficult because organizations waging CW have the talent to hide their identity. The attribution problem does cause difficulties throughout the JWT criterion and the probability of success criteria is not an exception. It makes it that much more important to evaluate all the indicators that could provide identification clues, which could include diplomatic conditions, intelligence sources, and forensic deconstruction of the cyber device used. Actors in cyber attacks do have signature ways in which they write code and the forensics intelligence is critical in cataloging the signatures in order to profile the attacks.

Cook compares the indistinctness in CW to identifying the Unabomber - eventually the identity is developed through the forensics profiling. In his words, "we can't always identify the agents of violence or their intentions."²⁷ Attribution is difficult even in "cases of non-cyberattack,"²⁸ but this difficulty doesn't negate the usefulness of JWT.

While the use of digital signatures to track cyber attacks and help avoid false targeting of civilians may appear attractive, the perception of it being a "big brother" issue and the fact that not all nations will comply with the regulations, based on its view of civil liberties, make it unlikely to succeed. Additionally, much like restricting the ownership of assault rifles in the

U.S., the only people affected are the ones already in compliance with the laws. Those who have the intent to do covert or clandestine harm on the Internet will never comply with digital signature or 'chips,' thus making attribution just as difficult as before. Furthermore, the probability of success measure would still require an evaluation of whether a response would help in culminating the aggression.

Crisp responds to the digital signature argument by falling back on the historical problem of identifying combatants in warfare, such as British service personnel living amongst the French in an undercover role during the Second World War. He states that the British put the local French citizens in harm's way and at risk of being mistaken for the British service personnel.²⁹ Perhaps a better and more recent situation is more helpful to understand the point of attribution - insurgency in Iraq.

During the war against Iraq, the insurgent groups intermingled with the local population and met in mosques and places of worship to conduct meetings that planned attacks against coalition forces. These situations created an extremely difficult situation for the coalition forces to discern between the innocent local civilians and the insurgents. When attacks did happen from a crowd of civilians or from a mosque, origination of the attack was difficult to determine, but through all-source intelligence and pattern of life investigations, the coalition forces became effective in identifying the sources of attacks and countering those attacks.

In investigating cyber attacks, it is unquestionable that the originator's identity can be elusive. However, much like the September 11th, 2001 attacks, identification of the perpetrators, no matter how elusive or time-intensive it might be to identify them, must happen so that further threats to national security are mitigated. The investigation to identify the 9/11 perpetrators and the insurgents attacking from Iraqi mosques took time and a lot of work. Nevertheless, it was

done despite the novelty of using commercial aircraft as weapons or using local Iraqis to mask the identity of those launching an attack. JWT and the criteria of probability of success are not negated by the novelty of the weapon used.

PROPORTIONALITY

Proportionality is important to understand prior to a state or nation initiating a war because it must “[weigh] the universal goods expected to result from it, such as securing the just cause, against the universal evils expected to result, notably casualties.”³⁰ Proportionality in JWT does not mean that responses must fit the 'an eye for an eye' type of response. The response from a victimized state may be more damaging than the initial attack, if it meets the previous criteria of the universal good outweighing the universal evils. In that respect, the response may cause more damage than the initial aggression, but if the response perpetuates a peaceful end to the aggression then the response could be said to be proportional. In this way, one could see the benefits of attribution within proportionality.

- Argument that cyber attacks never justify conventional weapons response

Lin and others provide an explanation of proportionality that isn't consistent with the above standard definition. They view proportionality as "the idea that it would be wrong to cause more harm in defending against an attack than the harm of the attack in the first place."³¹ Their reasoning is that there is no situation that would justify a conventional response to a cyber attack, because a conventional weapon would cause more damage than the cyber attack caused.³²

The argument is that in order to assess the proportionality of an attack, one must assess to what extent it was successful in hitting its target, and what damage the attack caused on the intended target and unintended targets (collaterally). Some use the Stuxnet attack on the Iranian

nuclear centrifuge process in an attempt to illuminate the issue.^{†††} They use the computer worm as an example of cyber attacks that spread and infect other more than just the intended target, with little damage to the actual target.³³ The Stuxnet worm targeted the Iranian Natanz uranium enrichment plant, which is known to be a closed circuit (or 'air gapped') network that could only be updated by the German Siemens' engineers. The updates were purportedly done via USB^{§§§} after the engineers connected to the Internet at their hotel with laptop computers.

The USBs were tainted with the Stuxnet worm and transferred the worm to the network at the Natanz plant, thereby jumping the air gap. Estimates credit Stuxnet with successfully damaging 1000 centrifuges. Unfortunately, whoever released the worm caused unintended infections throughout the world, which may have caused more harm than was caused to the Iranian nuclear program. Researchers found that "Stuxnet had a foothold on more than 100,000 computers, and they had no real idea what it was doing to them."³⁴ The originators of the destructive worm didn't know the extent of the damage done to the target until Stuxnet was released to unintended computers. The aftermath of the attack proved that Stuxnet hit its target system, but that it also caused unintended collateral damage without compelling Iran to end its nuclear ambitions.

The difficulty in not being able to determine the damage caused by a cyber attack limits the ability to respond with proportionality, and therefore this camp argues that JWT does not apply to CW. To them, cyber attacks leave too much room for interpretation since a victim of an attack could mistakenly think they were harmed more than they were actually harmed. That mistake could provoke a disproportional response, and thereby presenting ethical difficulties for the victim.³⁵ This is also why Dipert leans back to attribution while weighing the proportionality

^{†††} Stuxnet was a sophisticated worm that was believed to have infected PCs and damaged centrifuges at the Natanz uranium enrichment plant in central Iran.

^{§§§} Universal Serial Bus (USB) is an external bus standard that supports data transfer rates of 12 Mbps. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, and keyboards. USB also supports *Plug-and-Play* installation and *hot plugging*.

concerns by stating, "In the case of a cyberattack, the problem is uncertainty about who attacked us."³⁶ In order to meet the proportional criterion of JWT the counterstrikes must be aimed at the right enemy to determine if the universal good outweighs the universal evil of the response.

- Rebuttal

Proportionality within CW is problematic when intelligence is poor, but this problem is not new to war. As Cook points out, the U.S. wrongfully bombed the Chinese embassy in Belgrade during the air campaign over Kosovo based on bad intelligence.³⁷ More recently, the U.S. caused civilian casualties within Pakistan when it falsely identified a compound as an insurgent respite area. These unfortunate events unquestionably caused disproportionate damage due to poor identification of the aggressor force, which caused innocent individuals to die with no gain toward ending the conflicts. Cyber attacks, like any conventional attack, that are waged based on inadequate intelligence may produce a 90 percent confidence in the target, but be completely wrong based on errors in the information and subsequently cause damage to wrongfully targeted systems or people.

Even when the intelligence is accurate and the evidence stacks up to a high confidence level, the damage assessment of cyber attacks could be problematic, which subsequently makes assessing whether the attacks were proportional difficult. However, when physical effects are the purpose of the CW attack, the battle damage assessments (BDA) are not dissimilar to those of conventional weapons. For example - if a cyber attack targets a missile system similar to the Aegis scenario above, and the control panel for the missile system is being controlled by the cyber invader who fires a missile and hits the a target assigned by the cyber attacker, the BDA is known and thus the proportionality can be assessed. As with the Stuxnet worm BDA, the proportionality assessment heavily leans on the all-source intelligence mechanisms in order to

understand the damage to systems or information from the manipulation of industrial control systems.

In responding to a cyber attack, it is equally important to do the hard work and use the all-source intelligence apparatus to determine the aggressor. In developing the identity of the originator of a cyber attack, the victim must weigh the risk of being attacked again with an acceptable level of confidence in the identity of the aggressor. Cook uses an appropriate scenario where a nation destroys another nation's early-warning radars with a cyber attack, leaving the nation blind to air and missile attacks. The threat of air or missile attack from the aggressor nation is real and the victim nation cannot afford to be 100 percent confident in the attacker's identity before contemplating a response. Nor can the victim nation afford to wait and see if the aggressor nation launches missiles or aircraft to exploit the victim nation's blindness in that early-warning sector. In this case, it could be argued that the self-defense and protection of innocent people may warrant a conventional or cyber attack response with the aim of eliminating the air and missile threats, and probably outweighs the importance of a high level of attribution certainty for proportionality that ensure the ratio to universal good and evil is acceptable.³⁸

Cyber attacks on an aggressor nation like that in the above scenario may be appropriate, but may also unintentionally spread to innocent parties and therefore create proportionality concerns. This argument is, again, nothing new to JWT and warfare. Crisp responds to this argument by stating, "it has often been the case that those who unleash the dogs of war know full well that once released it may well be impossible to restrain them, and those who have been harmed find it hard to work out exactly how significant the harm in question is or may turn out to be."³⁹ War is unpredictable, so it is always difficult to judge proportionality, whether the weapon of choice is a conventional or cyber weapon. Proportionality assessments, applied to CW, provide a measure

to ensure acts of aggression in cyber are not waged without weighing the cost of launching a response to a cyber attack against the benefits it may produce, which may ultimately be a reinstatement of peace.

Chapter Three

CONCLUSION

Cyber operations, specifically cyber attacks, present new challenges to warfare, such as the speed and global delivery of lethal or non-lethal cyber weapons. Cyber attacks occur at the speed of light and can traverse the globe within milliseconds, delivering effects with some anonymity. Determining the source of attacks, managing proportionality of responsive weapons, and assessing the lethality of a cyber weapon are challenging the applicability of JWT to CW.

As history has shown, new technologies change the character of war, and it is undeniable that cyber weapons technology has and will continue to do so. Nevertheless, JWT remains applicable to assessing the justification for resorting to war and the conduct within war. Policies and regulations on Internet norms or conduct will be difficult to agree on, but as the U.N Charter expresses "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs."⁴⁰

That right to self-defense is what the U.S. is relying on to support its operations in cyberspace. President Obama has established the vision and hierarchy of command to posture the U.S. military to defend the nation in cyber. Whether that defense is through active or passive cyber operations does not matter. What will matter is justly responding to cyber attacks with either cyber or conventional weapons, and that is exactly why JWT must be applied to CW.

Both side of the argument to the application of JWT are worthy of reading to develop one's sense of the difficulties CW presents to JWT. The most prominent issues being discussed on both sides of the argument are whether cyber is or is not lethal, whether a probability of success measure can or can not be attained because of attribution problems, and whether proportionality can or can not be assessed with the attribution and lethality issues.

This paper contends that lethality is unquestionable due to the military, government, and financial world's reliance on networked computers that are vulnerable to exploitation and damage. The interconnection and susceptibility to exploitation, manipulation, and remote control from hostile actors allow weapon systems to be controlled with lethal consequences and critical government infrastructures to be manipulated with a result of causing deadly health hazards to humans. Attributing such acts of hostilities presents challenges across the JWT spectrum, but it is not dissimilar from historical examples that use JWT to determine the morality and ethical reasons for war.

The problem with attribution is conceded with exception. Attribution is difficult whenever new technologies change the character of war. As a mostly covert operation, CW is intended to go undetected until its intent is realized, and it is difficult to immediately know the source of the attack. Nevertheless, one must investigate by using all-source indicators and by conducting forensic analysis of the attack in order to assign attribution. Though the identity of an attack may take extensive time to answer and may very well go unanswered, the effort must be made so that, if a response is necessary, JWT can be applied to ensure just cause, probability of success, and proportionality are considered.

Colonel Cook is correct when he concludes that the "potential problems in the application of the JWT to CW represent differences in degree rather than in kind."⁴¹ Cyberspace is the medium in which cyber weapons are deployed under the umbrella of CW. As long as the U.S. applies the JWT criterion when confronted with a decision to respond to the threat or use of force by an antagonist, the weapon it chooses to deploy is secondary to the justification. After a careful review of the arguments, the application of JWT to CW is absolutely useful to evaluate the morality of actions within cyberspace.

Endnotes

- ¹ Matthew Humphries, "15-year-old hacks 259 websites in just 3 months," *geek.com*, 18 April 2012. <http://www.geek.com/articles/news/15-year-old-hacks-259-websites-in-just-3-months-20120418/>.
- ² Christopher Williams and Peter Foster, "Google Gmail cyber attack: 'Chinese spies had months of access'", *Telegraph*, 02 June 2011. <http://www.telegraph.co.uk/technology/google/8553131/Google-Gmail-cyber-attack-Chinese-spies-had-months-of-access.html>.
- ³ U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*. Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, 20 March 2009), I-7 (CH 1).
- ⁴ U.S. Department of Defense, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011), 2.
- ⁵ U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5.
- ⁶ Associated Press, "Hillary Clinton boasts of US cyberwar against al-Qaeda," *The Telegraph*, May 24, 2012, <http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html>.
- ⁷ "Fritz+Allhoff, Fritz Allhoff, online biography, last accessed 10 Feb 2013, <http://allhoff.org/>.
- ⁸ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ⁹ Randall Dipert, online biography, <http://www.dipert.org/>, Jan 13, 2013.
- ¹⁰ Paolo Passeri, "2012 Cyber Attacks Statistics," *Hackmageddon* (blog), January 17, 2013, <http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/>.
- ¹¹ Brian Orend, *Michael Walzer on War and Justice* (Montreal: McGill-Queen's University Press, 2000), 87.
- ¹² Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, Vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- ¹³ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ¹⁴ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ¹⁵ James Cook, "'Cyberation' and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics*, vol. 9, Issue 4, 2010, 411-423. <https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Cook.pdf>.
- ¹⁶ Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, Vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- ¹⁷ U.S. JCS, "Joint Publication 1," I-6.
- ¹⁸ Orend, 87.
- ¹⁹ Orend, 99.
- ²⁰ Orend, 99.
- ²¹ Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, Vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- ²² Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ²³ Steven J. Vaughan-Nichols, "What is a Botnet anyway?," *IT World* (blog), Feb 10, 2013, <http://www.itworld.com/security/74656/what-botnet-anyway>.
- ²⁴ Margaret Rouse, "IP spoofing (IP address forgery or a host file hijack)," *SearchSecurity; TechTarget*(blog), 10 Feb 2013, <http://searchsecurity.techtarget.com/definition/IP-spoofing>.
- ²⁵ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ²⁶ Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, Vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.

-
- ²⁷ Cook, 412.
- ²⁸ Cook, 412.
- ²⁹ Roger Crisp, "Cyberwarfare: No New Ethics Needed," *Practical Ethics*(blog), June 19, 2012, <http://blog.practicaethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/>.
- ³⁰ Orend, 87.
- ³¹ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?", *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ³² Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?", *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ³³ Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- ³⁴ Kim Zetter, "How digital detectives deciphered Stuxnet, the most menacing malware in history," *Wired*. July 7, 2011, <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/>.
- ³⁵ Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?", *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>.
- ³⁶ Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, Vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- ³⁷ Cook, 421.
- ³⁸ Cook, 416.
- ³⁹ Roger Crisp, "Cyberwarfare: No New Ethics Needed," *Practical Ethics* (blog), June 19, 2012, <http://blog.practicaethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/>.
- ⁴⁰ United Nations, *Charter of the United Nations and Statute of the International Court of Justice*. (New York: UN Publications, 2013), <http://www.un.org/en/documents/charter/chapter7.shtml>.
- ⁴¹ Cook, 422.

BIBLIOGRAPHY

- The Ashgate Research Companion to Ethics and International Relations*, s.v. "The Ethics of Global Governance and Global Governance of Ethics." accessed October 14, 2012, http://lomc.idm.oclc.org/login?url=http://www.credoreference.com/entry/ashgteir/the_ethics_of_global_governance_and_global_governance_of_ethics.
- Associated Press, "Hillary Clinton boasts of US cyberwar against al-Qaeda," *The Telegraph*, May 24, 2012, <http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html>.
- Belk, Robert and Matthew Noyes, "On the Use of Offensive Cyber Capabilities." Master's thesis, Harvard Kennedy School, 2012. <http://www.dtic.mil/docs/citations/ADA561817>.
- Chairman, Joint Chiefs of Staff, Joint Vision 2020. Washington, DC: U.S. Government Printing Office, June 2000.
- Conti, Gregory, James Caroland, Thomas Cook, and Howard Taylor. "Self-Development of Cyber Warriors." *Small Wars Journal*, November 2011. <http://www.dtic.mil/docs/citations/ADA552563>
- Cook, James, "'Cyberation' and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics*, vol. 9, Issue 4, 2010, 411-423. <https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Cook.pdf>.
- Davis, Maxie Y., "Ethical Considerations of Computer Network Attack in Information Warfare." Master's thesis, Marine Corps University, 2001. <http://www.dtic.mil/dtic/tr/fulltext/u2/a401168.pdf>.
- Dipert, Randall, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, vol. 9, Issue 4, 2010, *Special Issue: Ethics and Emerging Military Technologies*. <http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>.
- Friberg, Harry M., "U.S. Cyber Command Support to Geographic Combatant Commands." Master's thesis, U.S. Army War College 2001. <http://www.dtic.mil/dtic/tr/fulltext/u2/a543404.pdf>.
- Humphries, Matthew, "15-year-old hacks 259 websites in just 3 months," *geek.com*, 18 April 2012. <http://www.geek.com/articles/news/15-year-old-hacks-259-websites-in-just-3-months-20120418/>.
- International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*, 12 August 1949, 75 UNTS 287, accessed 21 January 2013, <http://www.unhcr.org/refworld/docid/3ae6b36d2.html>.

Libicki, Martin C., *Conquest in Cyberspace: National Security and Information Warfare*, New York: Cambridge University Press, 2007.

Orend, Brian, *Michael Walzer on War and Justice*. Montreal: McGill-Queen's University Press, 2000.

Owens, William A., Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC: National Research Council of the National Academies of Science, 2009.

Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 Jun 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>

Ried, Desmond A., "Cyber Sentries: Preparing Defenders to Win in a Contested Domain." Master's thesis, U.S. Army War College, 2012. <http://www.dtic.mil/dtic/tr/fulltext/u2/a561779.pdf>.

Senter, Jasper W., and Cayetano S. Thornton. "Information Technology (IT) Ethics: Training and Awareness Materials for the Department of the Navy." Master's thesis, Naval Postgraduate School, 2002. <http://www.dtic.mil/dtic/tr/fulltext/u2/a406010.pdf>.

United Nations, *Charter of the United Nations and Statute of the International Court of Justice*. (New York: UN Publications, 2013), <http://www.un.org/en/documents/charter/chapter7.shtml>.

U.S. Department of Defense, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011), 2.

U.S. Department of Defense, *Department of Defense Cyberspace Policy Report*. Washington, DC: Office of the Secretary of Defense, November 2011.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Office of the Secretary of Defense, July 2011.

U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*. Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, 20 March 2009), I-6 (CH 1).

U. S. Joint Chiefs of Staff, *Joint Pub 3-13*, Joint Doctrine for Information Operations (Ft Monroe, VA: Joint Warfighting Center, 1998).

Williams, Christopher and Peter Foster, "Google Gmail cyber attack: 'Chinese spies had months of access'", *Telegraph*, 02 June 2011. <http://www.telegraph.co.uk/technology/google/8553131/Google-Gmail-cyber-attack-Chinese-spies-had-months-of-access.html>.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 2011. <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/>.